Fake-Shops & Paket-SMS vor Ostern: 10 Warnsignale, 5 Sofortschritte

Cyberkriminelle nutzen verstärkt Online- Angebote und Paketbenachrichtigungen. Die WGV benennt typische Risiken und zeigt, wie sich Schäden vermeiden lassen.

P34/27 | 25. März 2026

- Vor Ostern steigt die Zahl der Online-Bestellungen – und damit auch das Risiko für Betrugsversuche
- Fake-Shops und Paket-SMS zählen zu den aktuell häufigsten Maschen
- Wer Warnsignale kennt und schnell reagiert, kann Schäden oft verhindern

Mit Blick auf Ostern steigt die Zahl der Online-Bestellungen – und damit auch das Risiko, Opfer von Cyberbetrug zu werden. Fake-Shops, betrügerische Paket-SMS und Phishing-Nachrichten gehören zu den häufigsten Maschen. Ziel ist es, Verbraucherinnen und Verbraucher zu schnellen Zahlungen oder zur Preisgabe sensibler Daten zu bewegen.

Online einkaufen, Geschenke bestellen oder Lieferungen verfolgen: Gerade vor Feiertagen spielt sich ein großer Teil des Alltags im Netz ab. Gleichzeitig wächst die Angriffsfläche für Cyberkriminelle. Viele Betrugsversuche wirken täuschend echt – und setzen gezielt auf Zeitdruck, Routinen und vermeintlich besonders günstige Angebote.

„Cyberkriminalität ist kein abstraktes Risiko mehr – sie passiert täglich und betrifft Menschen aller Altersgruppen“, sagt Alexander Birkle, Teamleiter in der Schadensabteilung der WGV Versicherung. Besonders häufig treten Betrugsfälle im Zusammenhang mit Onlinekäufen auf. „Viele Kundinnen und Kunden berichten, dass sie online bezahlt haben – aber die Ware nie ankam. Die Anbieterprofile verschwinden, das Geld ist verloren.“

Neben klassischen Fake-Shops nehmen auch sogenannte Smishing-Nachrichten zu. Dabei erhalten Betroffene SMS, die angeblich von Paketdiensten stammen und zu einer Sendungsverfolgung oder Adressbestätigung auffordern. Die enthaltenen Links führen häufig auf gefälschte Webseiten oder installieren Schadsoftware.

10 Warnsignale für Fake-Shops und Paket-SMS

- Ungewöhnlich günstige Preise deutlich unter Marktniveau
- Ware angeblich sofort verfügbar, obwohl sie anderswo ausverkauft ist
- Ausschließlich Vorkasse oder auffälliger Zahlungsdruck
- Internetadresse mit Schreibfehlern oder ungewöhnlicher Domain
- Fehlendes oder unvollständiges Impressum
- Gefälschte Gütesiegel oder Logos ohne Verlinkung
- Unpersönliche Anrede in Nachrichten

- Künstlicher Zeitdruck („nur noch heute“, „sonst Rücksendung“)
- Links in SMS oder E-Mails, die nicht zur offiziellen Seite führen
- Aufforderung zur Installation von Apps oder Eingabe sensibler Daten

Betrugsmaschen werden immer professioneller

Cyberkriminelle gehen zunehmend strategisch vor. Fake-Shops sind oft kaum noch von echten Online-Angeboten zu unterscheiden, während betrügerische Paket-SMS gezielt mit aktuellen Liefererwartungen arbeiten. Gerade vor Feiertagen nutzen Täter die hohe Bestellfrequenz und den Zeitdruck, um schnelle und unüberlegte Entscheidungen auszulösen.

„Viele Fälle beginnen mit einer scheinbar harmlosen Situation – etwa einer Lieferbenachrichtigung oder einem attraktiven Angebot“, sagt Alexander Birkle. „Doch hinter wenigen Klicks können sich erhebliche finanzielle und persönliche Risiken verbergen.“

5 Sofortschritte im Verdachtsfall

- Keine Links anklicken und keine Daten eingeben
- Sendungsstatus ausschließlich über offizielle Anbieter prüfen
- Online-Shops vor dem Kauf überprüfen
- Bei bereits erfolgter Zahlung umgehend Bank oder Zahlungsdienst kontaktieren
- Verdächtige Nachrichten beim jeweiligen Anbieter melden

Noch gravierender sind Fälle, in denen persönliche Daten missbraucht oder Betroffene gezielt unter Druck gesetzt werden. Neben finanziellen Schäden können solche Vorfälle auch rechtliche und emotionale Folgen haben.

„Wir erleben immer wieder, dass digitale Angriffe weit über den eigentlichen Schaden hinausgehen“, so Birkle. „Umso wichtiger ist es, im Ernstfall schnell Unterstützung zu bekommen – technisch, juristisch und auch persönlich.“

Gerade bei Online-Betrug oder Identitätsdiebstahl stehen viele Betroffene vor der Frage, wie sie sich wehren können und welche Schritte sinnvoll sind. Unterstützung bieten hier beispielsweise rechtliche Absicherung und Lösungen zum Schutz vor Cyberrisiken.

Aufklärung bleibt angesichts zunehmender Betrugsversuche ein zentraler Baustein der Prävention. . Wer typische Warnsignale kennt und im Zweifel genau hinschaut, kann sich wirksam schützen – nicht nur zur Osterzeit.

Unterstützung im Ernstfall

Wenn Verbraucher Opfer von Online-Betrug werden, kommt es vor allem auf schnelle und kompetente Hilfe an. Neben der Sicherung finanzieller Schäden spielen auch rechtliche Fragen eine zentrale Rolle – etwa bei der Durchsetzung von Ansprüchen oder dem Umgang mit Identitätsdiebstahl.

Die WGV Versicherung bietet mit ihrer Rechtsschutzversicherung und der Cyberversicherung Lösungen, die Betroffene in solchen Situationen unterstützen können. Sie unterstützen unter anderem dabei, rechtliche Schritte zu klären und digitale Schäden zu bewältigen.

Über die WGV

Seit 1921 versorgt die WGV Versicherung ihre Kunden mit umfassenden Versicherungslösungen. Mehr als 1.200 Mitarbeiter arbeiten bei der WGV deutschlandweit daran, Privat- und Kommunalkunden bedarfsgerechten Versicherungsschutz anzubieten. Die WGV Versicherung verfügt über 1,3 Mrd. € Eigenkapital und verwaltet über 6,3 Mio. Versicherungsverträge mit einem Beitragsvolumen von über 1 Mrd. €. Neben der Württembergische Gemeinde-Versicherung a.G. als Mutterunternehmen, gehören zur WGV Gruppe die WGV-Beteiligungsgesellschaft GmbH, die WGV-Versicherung AG sowie die WGV Holding AG mit der WGV Rechtsschutz-Schadenservice GmbH, der WGV-Lebensversicherung AG und der WGV-Informatik und Media GmbH. Weitere Informationen unter www.wgv.de.

Ansprechpartner:

Unternehmenskommunikation
Alissa Nefzer
Württembergische Gemeinde-Versicherung a.G.
70178 Stuttgart
presse@wgv.de
www.wgv.de